Management System: Safeguards and Security

Subject Area: Information Security

Procedure 3: Managing a Site Operations Security (OPSEC) Program

Issue Date:	Lead Subject Matter Expert:	Management System Owner:
08/23/2012	Pat Vent or Shaun Meadows	John Sattler

1.0 Applicability

This procedure is applicable to all EMCBC Federal and contractor personnel with responsibilities for implementing an OPSEC Program, to include maintenance of an OPSEC Plan, development of a Local Threat Assessment, and provision of OPSEC Awareness training.

.

2.0 Required Procedure

The initial requirement in development and implementation of an OPSEC Program is identifying and understanding the organization's Critical Information (CI). The next requirement is identifying and understanding the threats to the theft, unauthorized release, or unauthorized manipulation/distortion of the CI. The final requirement is the identification and implementation of methods to mitigate the risks to the CI, such as ongoing OPSEC awareness activities, and reviews of information prior to its being made publicly available.

Step 1	The EMCBC Director appoints an individual to serve as the OPSEC Program Manager.
Step 2	In consultation with the EMCBC Assistant Directors (ADs), or their designees, the OPSEC Program Manager develops a list of the EMCBC's CI by topic.
Step 3	The OPSEC Manager evaluates the need for a standing OPSEC Working Group or Committee based upon input from the ADs. If this evaluation determines such a body is needed, representatives from the various EMCBC offices are solicited and appointed. The CI List developed in Step 2 should be at the forefront of any deliberations by the OPSEC Working Group, but is subject to revision whenever required.
Step 4	The OPSEC Manager is responsible for ensuring a Local Threat Statement is developed, and annually reviewed and updated as needed.
Step 5	The OPSEC Program Manager maintains contact with local representatives of local and Federal law enforcement organizations, and with the DOE Office of

	Counterintelligence. Input is solicited from these entities in the development of the Local Threat Statement.
Step 6	The OPSEC Manager develops OPSEC awareness messages for incorporation into various security briefings, including initial, comprehensive and refresher briefings. Other tools are used to promote OPSEC awareness, such as the placement of posters, presentation of videos, and emailed news stories.
Step 7	The OPSEC Manager consults with personnel responsible for the reviews of information for classification, public affairs, and Freedom of Information/Privacy Act responses to ensure that CI is not released to the public.

3.0 References

- DOE O 471.6, Information Security
- National Security Decision Directive 298, National Operations Security Program

4. Records Generated

The records table identifies those records generated during the work process described in any controlled document/procedure that shall be maintained to document activities or preserve historically valuable information after the work process is completed.

Records generated through implementation of this procedure are identified as follows, and are maintained by the Office of Technical Support & Asset Management in accordance with the EMCBC Organizational File Plan:

Records Category Code	**Records Title**	**Responsible Organization**	**QA Classification** **(Lifetime, Non-Permanent or N/A)**
ADM 18-08.1-B	OPSEC Program Management Records	Office of Technical Support & Asset Management	NA